



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/589,747	06/09/2000	Neil Gilbert Siegel	199.38513X00	1612

7590

09/09/2002

Patent Counsel
TRW Inc
Space & Electronics Group
One Space Park E2/6072
Redonda Beach, CA 90278

EXAMINER

BACKER, FIRMIN

ART UNIT

PAPER NUMBER

3621

DATE MAILED: 09/09/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/589,747

Applicant(s)

SIEGEL ET AL.

Examiner

Firmin Backer

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 June 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

DETAILED ACTION

This is in response to a letter for patent filed on June 9th, 2000 in which claims 1-41 are presented for examination. Claims 1-41 are pending in the letter.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kung (U.S. Patent No. 5,421,594) in view of IBM disclosure bulletin (U.S. No. NN880530).

3. As per claims 1, Kung teaches a method of administering access and security (*apparatus and method of authenticating user*) on a network (*networked*) having a plurality of computers (*distributed computing system*) (*see abstract, fig 1 and 2*), comprising installing an encrypted password file (*storing on a database, 19b, user ids and encrypted passwords*) on each computer (*user computer, 11, remote computer, 13*) of the plurality of computers in the network, wherein the encrypted password file includes a plurality of user identifications (*user ids*), associated encrypted passwords (*encrypted passwords*) and associated privileges for each authorized user allowed access to the plurality of computers and the network (*see abstract, fig 4, column 2 lines*

Art Unit: 3621

12-46), a password entered by a user (*user enter appropriate ID and password*) when the user logs into a computer of the plurality of computers on the network, (*see fig 2,3 column 4 lines 30-48*) checking (*comparing*) for a match between the user identification (*user, ID*) and encrypted password (*password*) entered by the user and the plurality of user identifications and encrypted passwords stored in the encrypted password file (*see fig 4, column 5 lines 38-53, 6 lines 18-50*), enabling access (*access granted*) to data and software (*software program, 32*) contained on the computer and the network permitted by the associated privileges for the user when a match is found on the encrypted password file (*see fig 4, column 5 lines 54-6 line 38*), and filtering and displaying messages (*message is sent to user's workstation, 11*) to the user permitted by the associated privileges when a match is found on the encrypted password file (*see column 4 line60-5 line 18*). Kung fails to teach and inventive concept that includes a one-way encrypted password. However, in the IBM disclosure, and inventive concept that include a one-way encrypted password is disclosed (*see IBM disclosure*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Kung's inventive concept to include a one-way encrypted password because this would have reduced the period of time that the identification information is exposed during the identification function thereby resulting in better security.

4. As per claims 2, Kung teaches a method wherein the associated privileges contained in the encrypted password file indicate the security level and access privileges of the user identification for access to software, data and messages contained in the computer, the network, and transmitted over the network (*see column 4 line60-5 line 18*).

5. As per claims 3, Kung teaches a method wherein when one or more attempts of the user entering a user identification and encrypted password have failed to match the plurality of user identifications and encrypted passwords contained in the encrypted password file, the method further comprising: transmitting to a systems administrator or security officer by the computer a notification of the failure to provide a encrypted user identification and password that matches a user identification and encrypted password stored on the encrypted password file (*see fig 2,3 column 4 lines 30-48*).

6. As per claims 4, Kung teaches a method further comprising locking, upon request by the systems administrator or security officer, the computer being accessed by the user having at least one failed attempt at entering a user identification and encrypted password so as to permit only access to a login screen by the user (*see abstract, fig 4, column 2 lines 12-46*).

7. As per claims 5, Kung teaches a method further comprising spoofing, upon request by the systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user (*see column 4 line 60-5 line 18*).

8. As per claims 6, Kung teaches a method further comprising disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system (*see fig 4, column 5 lines 54-6 line 38*).

9. As per claims 7, Kung teaches a method further comprising deleting, upon request by the systems administrator or security officer, a plurality of files stored in the computer system (*see abstract, fig 4, column 2 lines 12-46*).

10. As per claims 8, Kung teaches a method further comprising displaying to a screen on the computer system a request for re-authentication at the direction of a system administrator or a security officer (*see fig 2,3 column 4 lines 30-48*).

11. As per claims 9, Kung teaches a method wherein the request for re-authentication comprises displaying a login screen having a position for entry of the user identification and password (*see fig 4, column 5 lines 54-6 line 38*).

12. As per claims 10, Kung teaches a method wherein the user identification is a role or title indicative of a level of authority of the user (*see fig 2,3 column 4 lines 30-48*).

13. As per claims 11, Kung teaches a method further comprising accessing a master password file on a computer system accessible by the systems administrator or security officer; encrypting the password; and searching the master password file for a match of the user identification and encrypted password (*see abstract, fig 4, column 2 lines 12-46*).

Art Unit: 3621

14. As per claims 12, Kung teaches a method further comprising disabling the computer system, or spoofing the user, or locking the computer system when a match is not found for the user identification and encrypted password in the master password file (*see fig 4, column 5 lines 38-53, 6 lines 18-50*).

15. As per claims 13, Kung teaches a method wherein after the user has entered the user identification and encrypted password and the user identification and password has matched that found in the encrypted password file, further comprising entering a new password by the user, re-authenticating the user identification and password stored on the master password file, encrypting the new password; and replacing the user identification and password with the encrypted user identification and the new encrypted password in the master password file (*see fig 4, column 5 lines 38-53, 6 lines 18-50*).

16. As per claims 14, Kung teaches a method further comprising: attaching the master password file to a message, encrypting the message using a private key and passphrase available only to the systems administrator or security officer; and transmitting the message to the plurality of computers (*see fig 4, column 5 lines 38-53, 6 lines 18-50*).

17. As per claims 15, Kung teaches a method further comprising decrypting the message using a public key corresponding to the private key; reporting to the system administrator or security officer a failure to decrypt the message; and replacing the encrypted password file with the decrypted master password file (*see column 4 line 60-5 line 18*).

18. As per claims 16, Kung teaches a method further comprising detecting an anomalous event in a computer of the plurality of computers; and reporting the anomalous event to a system administrator or security officer (*see fig 2,3 column 4 lines 30-48*).

19. As per claims 17, Kung teaches a method wherein the anomalous event comprise: the user has exceeded the number of allowable unsuccessful login attempt; a change in the users associated privileges has occurred, a system disable operation was initiated by the user; a user's password has expired, a message was rejected due to an invalid digital signature, a request for remote user re-authentication has been received by the system administrator or security officer, a request for a remote user lockout has been received by the system administrator or security officer; and a request for remote loading passwords has completed successfully on the system administrator or security officer (*see abstract, fig 4, column 2 lines 12-46*).

20. As per claims 18, Kung teaches a method further comprising deleting a plurality of files on the computer and disabling the computer in response to an anomalous event when requested by the system administrator or security officer or when an immediate shutdown in requested by the user (*see fig 4, column 5 lines 38-53, 6 lines 18-50*).

21. As per claims 19, Kung teaches a method further comprising disabling the computer system, or spoofing the user, or locking the computer system when an anomalous event occurs (*see fig 4, column 5 lines 54-6 line 38*).

Art Unit: 3621

22. As per claims 20 and 31, Kung teaches a system to administer access and security (*apparatus and method of authenticating user*) on a network (*networked*) having plurality of computers (*distributed computing system*) (*see abstract, fig 1 and 2*), comprising a encrypted password file (*storing on a database, 19b, user ids and encrypted passwords*) on each computer of the plurality computers (*user computer, 11, remote computer, 13*) in the network, wherein the encrypted password file includes plurality of user identifications (*user ids*), associated encrypted passwords (*encrypted passwords*) an associated privileges for each authorized user allowed access to the plurality computers and the network (*see abstract, fig 4, column 2 lines 12-46*), a user login module to receive a user identification or role and password from a user and login the user when a match is found in the encrypted password file(*see fig 2,3 column 4 lines 30-48*); and a channel monitoring and filtering module to monitor and receive broadcast c multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message (*see column 4 line60-5 line 18*). Kung fails to teach and inventive concept that includes a one-way encrypted password. However, in the IBM disclosure, and inventive concept that include a one-way encrypted password is disclosed (*see IBM disclosure*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Kung's inventive concept to include a one-way encrypted password because this would have reduced the period of time that the identification information is exposed during the identification function thereby resulting in better security.

Art Unit: 3621

23. As per claims 21 and 32, Kung teaches a system further comprising a password management module to update and insure that all the computers in the network contain the same encrypted password file (*see fig 2,3 column 4 lines 30-48*).

24. As per claims 22 and 33, Kung teaches a system further comprising a remote auditing module to monitor and process anomalous events which may occur on the computer (*see fig 4, column 5 lines 54-6 line 38*).

25. As per claims 23 and 34, Kung teaches a system wherein the anomalous events comprise: the user has exceeded the number of allowable unsuccessful login attempts; a change in the users associated privileges has occurred, a system disable operation was initiated by the user; a user's password has expired, a message was rejected due to an invalid digital signature, a request for remote user re-authentication has been received by the systems administrator or security officer, a request for a remote user lockout has been received by the system administrator or security officer; and a request for remote loading passwords has completed successfully on the system administrator or security officer (*see fig 2,3 column 4 lines 30-48*).

26. As per claims 24 and 35, Kung teaches a system further comprises a remote control module to enable a systems administrator or security officer to take appropriate action when an event transpires, wherein the event is an anomalous event (*see fig 2,3 column 4 lines 30-48*).

Art Unit: 3621

27. As per claims 25 and 36, Kung teaches a system wherein the appropriate action comprises disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system; and deleting, upon request by a systems administrator or security officer, a plurality of files stored in the computer (*see abstract, fig 4, column 2 lines 12-46*).

28. As per claims 26 and 37, Kung teaches a system wherein the appropriate action comprises spoofing, upon request by a systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user (*see fig 4, column 5 lines 38-53, 6 lines 18-50*).

29. As per claims 27 and 38, Kung teaches a system wherein the appropriate action comprises: locking the computer, upon request of a systems administrator or security officer, and displaying a login screen for the user to re-authenticate the user identification and password (*see fig 2,3 column 4 lines 30-48*).

30. As per claims 28 and 39, Kung teaches a system further comprising an authentication module to re-authenticate the user after the user login module has found a match in the encrypted password contained in the computer by checking the user identification and password against a master password file stored in a computer accessible by a systems administrator or security officer (*see fig 4, column 5 lines 38-53, 6 lines 18-50*).

Art Unit: 3621

31. As per claims 29 and 40, Kung teaches a system wherein the password management module attaches a master password file containing a complete user identifications, associated encrypted passwords and associated privileges to a message, encrypts the message using a private key and passphrase for the system administrator or security officer and broadcasts the message to all users (*see fig 4, column 5 lines 54-6 line 38*).

32. As per claims 30 and 41, Kung teaches a system wherein the password management module decrypts the message using a public key associated with the private key, replaces the encrypted password file when decryption of the message is successful and reports a failure to the system administrator or security officer when the decryption is not successful (*see fig 4, column 5 lines 38-53, 6 lines 18-50*).

Conclusion

33. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. *Kaufman (U.S. Patent No. 6,178,508) teaches in a system, an authorized user must enter a password which, when hashed, can be found in the unencrypted header file. If the entered password is found in the file, the user is authorized access to the protected encrypted data.*

Art Unit: 3621

b. *Angelo et al (U.S. Patent No. 5,953,422) teach in a method wherein a user verification process is then performed on the network password to determine which, if any, access privileges have been accorded the network user. As an example, access to certain pieces of data can be limited to a specified user on a specified network node. Numerous other uses are contemplated for the network password. The password can be utilized: to decrypt or encrypt data on the server hard drive (similar to a session key), as part of a public key/private key pair, or as part of a split key or forced key pair. Such uses permit the server hard drive(s) or other network resources to be securely compartmentalized with the option to have multiple user levels.*

c. *Funk Paul (U.S. Patent No. 5,521,779) teaches a method that employs a challenge and response handshake technique that allows a server to authenticate a client based on a password. The method provides the server with a challenge signal generator, such as a number generator that generates numbers, or electrical signals representative of numbers. The method further provides the system with a database of authentication values, or electrical signals representative of authentication values, where each authentication values corresponds to a valid password.*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammel can be reached on (703) 305-9768. The fax phone numbers for the

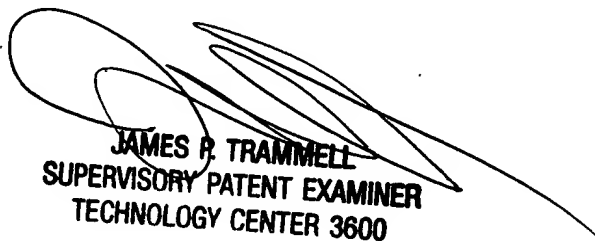
Art Unit: 3621

organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.



Firmin Backer
August 29, 2002



JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600